



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/758,818

01/16/2004

Raynold M. Kahn

PD-200292

6585

20991 7590 08/20/2007

THE DIRECTV GROUP INC
PATENT DOCKET ADMINISTRATION RE/R11/A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER

SCHMIDT, KARI L

ART UNIT

PAPER NUMBER

2139

MAIL DATE

DELIVERY MODE

08/20/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/758,818

Applicant(s)

KAHN ET AL.

Examiner

Kari L. Schmidt

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 January 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-44 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date See Continuation Sheet.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- ☐ Notice of Informal Patent Application
- ☐ Other: _____.

Art Unit: 2139

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-12 are rejected under 35 U.S.C. 102(b) as being anticipated by Son et al. (US 2001/0017920 A1).

Claim 1 & 7

Son discloses a method and an apparatus of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising:

(a) receiving an encrypted media encryption key at the host receiver ([0028-0029]: "when remote server receives a request for transmission of the video program from a subscriber... (remote server within a distribution center of video-on demand source).. video program is encrypted by a video on-demand source to generate an encrypted program in a first encrypted form..") ;

(b) decrypting the encrypted media encryption key at the host receiver ([0029]: "the remote server responds by first decrypting the video program from the first encrypted form..");

Art Unit: 2139

- (c) re-encrypting the decrypted media encryption key at the host receiver using a pairing key ([0029]: "the video program is decrypted to the remote server re-encrypts the video program into a second encrypted form using a second key");
- (d) transferring the re-encrypted media encryption key from the host receiver to the client receiver ([0031]: host receiver = remote server within the distribution center and client receive = subscriber; video program is re-encrypted the re-encrypted program in the second encrypted form.. distributed to the subscriber");
- (e) decrypting the re-encrypted media encryption key at the client receiver using the pairing key (Figure 5A (510 to 512));
- (f) receiving encrypted program materials from the broadcast system at the host receiver (Figure 5A (514));
- (g) transferring the encrypted program materials from the host receiver to the client receiver (Figure 5A (516 to 520)); and
- (h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key (Figure 5A (520)).

Claim 2 & 8

Son discloses the method and the apparatus of claim 1, further comprising decrypting the encrypted program materials at the host receiver using the decrypted media encryption key ([0029-0030]: "remote sever responds by first decrypting the video program from the first encrypted form.. using the private key").

Art Unit: 2139

Claim 3 & 9

Son discloses the method and the apparatus of claim 1, further comprising receiving the pairing key from the broadcast system at both the host receiver and the client receiver ([0029 & 0034]: "pairing keys is from the public key encryption system (public/private keys)... remote server decrypts the video program from the first encrypted form.. a first key is may be used for decryption, such key may have been received from the video-on demand source.. ").

Claim 4 & 10

Son discloses the method and the apparatus of claim 3, wherein the receiving step comprises: receiving the pairing key from the broadcast system at the host receiver, wherein the pairing key is encrypted; and decrypting the pairing key at the host receiver using a receiver key uniquely associated with the host receiver ([0029-0034]: first key is may be used for decryption and such key have been received from the video on-demand source... video program is decrypted the remote server re-encrypts the video program into a second encrypted form using a second key... encrypted program in a first encrypted form..")

Claim 5 & 11

Son discloses the method and the apparatus of claim 3, wherein the receiving step comprises: receiving the pairing key at the client receiver, wherein the pairing key is encrypted; and decrypting the pairing key at the client receiver using a receiver key uniquely associated with the client receiver ([0039-0042]: "

Art Unit: 2139

private key transported from source (server); public key is for encrypting and private key is for decrypting; video program is encrypted by a video on-demand source to generate an encrypted program in a first encrypted form. The encrypted program is transported from the video on-demand source to a remote server.. a key to decrypt the encrypted program.. the private key may be transported from the source to the server.. ").

Claim 6 & 12

Son discloses the method and the apparatus of claim 5, further comprising: receiving the pairing key from the broadcast system at the host receiver; and transferring the pairing key from the host receiver to the client receiver ([0031-0041]: "remote server = host receiver: responds by first decrypting the video program from the first encrypted form. After decrypted the remote server re-encrypts the video program into a second encrypted form using a second key... after being re-encrypted distributed to the subscriber stations.. at the subscriber stations the multiplexed signal is demultiplexed to isolate the re-encrypted program in the second encrypted form the re-encrypted program is decrypted form the second encrypted form to generate the unencrypted video program and then the video program is display (Figure 5A)").

Art Unit: 2139

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 13-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Son et al. (US 2001/0019720 A1) in view of Mas Ribes (US 2006/0179489 A1).

Son discloses a method and an apparatus of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption, comprising: (a) receiving an encrypted media encryption key at the host receiver ([0028-0029]: "when remote server receives a request for transmission of the video program from a subscriber... (remote server

within a distribution center of video-on demand source).. video program is encrypted by a video on-demand source to generate an encrypted program in a first encrypted form..”) ;(b) decrypting the encrypted media encryption key at the host receiver ([0029]: “ the remote server responds by first decrypting the video program from the first encrypted form..”); (c) re-encrypting the decrypted media encryption key at the host receiver using a pairing key ([0029]: “ the video program is decrypted to the remote server re-encrypts the video program into a second encrypted form using a second key”); (d) transferring the re-encrypted media encryption key from the host receiver to the client receiver ([0031]: host receiver = remote server within the distribution center and client receive = subscriber; video program is re-encrypted the re-encrypted program in the second encrypted form.. distributed to the subscriber”); (e) decrypting the re-encrypted media encryption key at the client receiver using the pairing key (Figure 5A (510 to 512));(f) receiving encrypted program materials from the broadcast system at the host receiver (Figure 5A (514)); (g) transferring the encrypted program materials from the host receiver to the client receiver (Figure 5A (516 to 520)); and (h) decrypting the encrypted program materials at the client receiver using the decrypted media encryption key (Figure 5A (520)).

Son doesn't specifically state a method and an apparatus using conditional access module associated with the host receiver of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption.

Art Unit: 2139

Mas Ribes discloses a method and an apparatus of distributing program materials received from a broadcast system between a host receiver and a client receiver for remote decryption.

Regarding claims 13-44, Mas Ribes discloses a multi-layered conditional access method for processing a protected digital content between a content protector, an intermediate receiver, and final destination means. The method comprises: a) encryption by the content protector of a key or keys for accessing protected digital content, b) the transmission from the content protector for the intermediate receiver of the encrypted key or keys, c) the decryption and re-encryption of the key or keys by the intermediate receiver, d) the transmission of the re-encrypted key or keys to a final destination device, and e) the decryption of the re-encrypted key or keys by the final destination device (Abstract).

Conditional Access Modules can be smart cards, which act in the system as delegates of the content protector within remote system. ([0039]).

It would have been obvious to one of ordinary skill in the art at the time of invention to have a conditional access module for remote decryption between the host receiver and client receiver. Since conditional access modules performs cryptographic and condition verification operations to protect TV content ([0039], Abstract), which Mas Ribes teaches.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Art Unit: 2139

Maillard (US 7, 191, 335 B1) teaches method and apparatus for encrypted transmission.

Fransdonk (US 6, 961, 858 B2) teaches a method and system to secure content for distribution via a network.

Ezaki (US 7, 035, 827 B2) teaches a content receiving apparatus and method, storage medium, and server.

Viljoen et al (US 2006/0168663 A2) teaches secure transaction protocol.

Koga, Keiichiro. Security for Information Data Broadcasting System with Conditional-Access Control. IEEE: 1995.

EBU Project Group B/CA. Functional model of a conditional access system. EBU Technical Review: 10 June 1995.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kari L. Schmidt whose telephone number is 571-270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KS



TAGHI ARANI
PRIMARY EXAMINER

5/26/07

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date
:3/20/2007,8/1/2005,
4/1/2005,2/23//2005,1/16/2004,9/25/2006,5/3/2006,3/3 0/2006,1/12/2006,4/20/2005,1/21/2005,10/13/2004,10/12/2004.